

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2013/03

Lecteur RFID LXS W33-E/PH5-7AD
Version 1.0

Paris, le 19 mars 2013

Le directeur général de l'agence nationale de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]



Avertissement

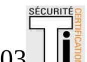
Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié. C'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr



Référence du rapport de certification **ANSSI-CSPN-2013/03**
Nom du produit **Lecteur RFID LXS W33-E/PH5-7AD**
Référence/version du produit **1.0**
Catégorie de produit **Matériel et logiciel embarqué**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)***
Développeur **Systèmes et Technologies Identification (STid)** **20, Parc d'activités des Pradeaux** **13850 Gréasque** **France**
Commanditaire **Systèmes et Technologies Identification (STid)** **20, Parc d'activités des Pradeaux** **13850 Gréasque** **France**
Centre d'évaluation **CEA - LETI** **17, rue des Martyrs** **38054 Grenoble Cedex 9**

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est le « lecteur RFID LXS W33-E/PH5-7AD, version 1.0 » développé par la société Systèmes et Technologies Identification (STid).

Ce produit est un lecteur de badge, avec capteur anti-arrachement, destiné à contrôler l'accès à une zone donnée. Il s'agit d'un lecteur RFId de technologie 13,56MHz, conforme aux normes RFId ISO 14443-A et 14443-B. Il implémente en particulier toutes les fonctionnalités de la famille Mifare de NXP.

Le lecteur est géré par une unité de traitement logique (ci-après UTL ou contrôleur) via une liaison série RS485 et un protocole propriétaire SSCP V2. Ce protocole permet d'effectuer une authentification entre l'UTL et le lecteur de badge et assure la sécurité des communications entre ces deux éléments.

Ce produit s'inscrit dans l'architecture n°2 définie dans le chapitre 4.3 du guide de sécurité des technologies sans-contact pour le contrôle des accès physiques [GUIDES-ANSSI] où le lecteur dispose d'une liaison sécurisée avec le badge et avec l'UTL.

1.2. Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1. Catégorie du produit

☐ 1 - détection d'intrusions
☐ 2 - anti-virus, protection contre les codes malicieux
☐ 3 – firewall
☐ 4 - effacement de données
☐ 5 - administration et supervision de la sécurité
☐ 6 - identification, authentification et contrôle d'accès
☐ 7 - communication sécurisée
☐ 8 - messagerie sécurisée
☐ 9 – stockage sécurisé
☒ **10 - matériel et logiciel embarqué**
☐ 99- Autres

1.2.2. Identification du produit

La version certifiée du produit est identifiable par le biais d'une étiquette située à l'intérieur du lecteur.



1.2.3. Services de sécurité

Les services de sécurité fournis par le produit faisant l'objet de l'évaluation sont :

- l'authentification mutuelle du lecteur et du contrôleur / UTL ;
- la sécurisation de la communication entre le lecteur et le contrôleur.

Par ailleurs, l'interface de communication entre le badge et le lecteur, gérant notamment l'identification et l'authentification du badge, n'a pas été évaluée. Cependant, le choix d'un badge certifié permettra de couvrir les besoins de sécurité vis-à-vis de cette interface (voir §2.3.12.2).

1.2.4. Configuration évaluée

Dans le cadre de l'évaluation, le mécanisme de détection d'arrachement du lecteur a été activé.

2. L’évaluation

2.1. Référentiels d’évaluation

L’évaluation a été menée conformément à la Certification de sécurité de premier niveau. Les références des documents se trouvent en annexe 2.

2.2. Charge de travail prévue et durée de l’évaluation

La durée de l’évaluation a été conforme à la charge de travail prévue lors de la demande de certification, elle-même conforme à la charge de travail préconisée dans [CSPN] pour un produit comportant des mécanismes cryptographiques, soit 35 hommes x jours.

2.3. Travaux d’évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [CDS] fournie en entrée de l’évaluation. Ces précisions sont issues du [RTE] élaboré par l’évaluateur suite à ses travaux.

2.3.1. Fonctionnalités, environnement d’utilisation et de sécurité

2.3.1.1. Spécification de besoin du produit

Conforme à la cible de sécurité [CDS] (chapitre 3 « Argumentaire du produit »).

2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre 5 « Biens sensibles devant être protégés par le produit »).

2.3.1.3. Description des menaces contre lesquelles le produit apporte une protection

Conforme à la cible de sécurité [CDS] (chapitre 6 « Description des menaces »).

2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre 7 « Description des fonctions de sécurité du produit »).

2.3.1.5. Utilisateurs typiques

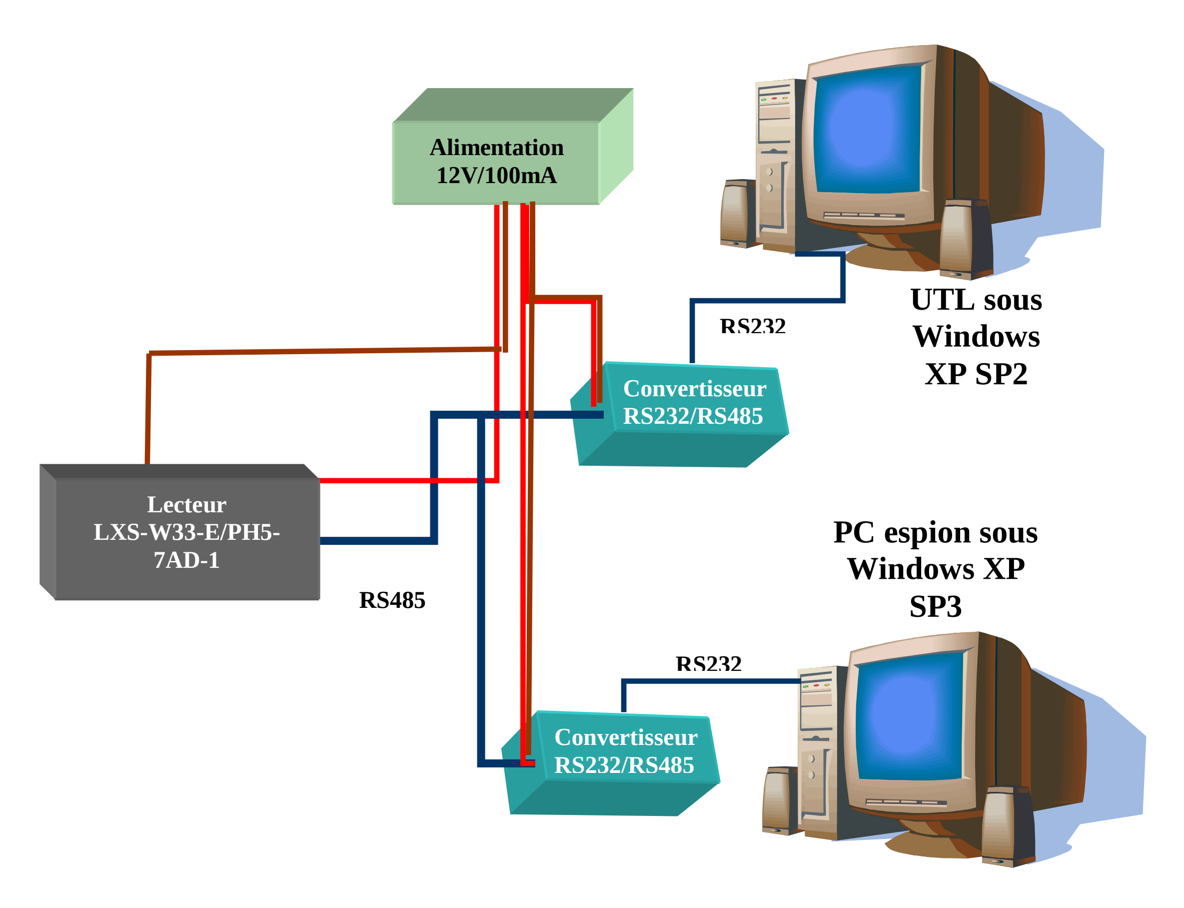
Conforme à la cible de sécurité [CDS] (chapitre 3.6 « Description des utilisateurs typiques concernés »).



2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

La plate-forme de test est décrite dans la figure suivante :



L'UTL utilisée pour les tests est un PC sous Windows XP Service Pack 2.
Pour effectuer les tests anti-rejeu, les tests d'usurpation du lecteur ou de déni de service du lecteur, l'évaluateur a mis un PC espion en parallèle sur la liaison RS485 entre l'UTL et le lecteur

2.3.2.2. Particularités de paramétrage de l'environnement

Afin de tester la fonctionnalité d'anti-arrachement, et conformément à l'usage du produit, le lecteur a été fixé sur un mur.

2.3.2.3. Options d'installation retenues pour le produit

Dans le cadre de l'évaluation, le mécanisme de détection d'arrachement a été activé.

2.3.2.4. Description de l'installation et des non-conformités éventuelles

Sans objet.

2.3.2.5. Durée de l'installation

L'installation a nécessité moins d'une journée.

2.3.2.6. Notes et remarques diverses

L'installation est simple et suffisamment documentée.

2.3.3. Analyse de la documentation

L'évaluateur a eu accès à la documentation technique du produit [GUIDES]. La documentation est claire et aucune non-conformité n'a été relevée.

2.3.4. Revue du code source (facultative)

Les évaluateurs ont eu accès à la partie du code source traitant de la gestion des clés. Le code est clair et les bonnes pratiques de programmation y sont globalement respectées.

2.3.5. Fonctionnalités testées

Fonctionnalité	Résultat
Identification, authentification et contrôle d'accès	**Réussite**
Détection d'arrachement	**Réussite**
Effacement des données	**Réussite**
Communication sécurisée	**Réussite**
Stockage sécurisé	**Réussite**

2.3.6. Fonctionnalités non testées

L'interface de communication RFID entre le lecteur et le badge n'a pas été évaluée.

2.3.7. Synthèse des fonctionnalités testées / non testées et des non-conformités

Sans objet.

2.3.8. Avis d'expert sur le produit

Le fonctionnement du produit est conforme à ses spécifications fonctionnelles.

2.3.9. Analyse de la résistance des mécanismes et des fonctions

2.3.9.1. Liste des fonctions et des mécanismes testés

Fonction et mécanisme
Authentification mutuelle du lecteur et de l'UTL
Sécurisation des échanges entre le lecteur et l'UTL
Détection d'arrachement du lecteur

2.3.9.2. Avis d'expert sur la résistance des mécanismes

La phase d'authentification permet de garantir la non-usurpation d'identité du lecteur ou de l'UTL mais le système n'est pas protégé contre un éventuel déni de service.
L'analyse du mécanisme de détection d'arrachement a montré qu'il était contournable. Cependant, le contournement de cette fonctionnalité n'a pas suffit à mettre à mal les biens sensibles protégés par le produit.

2.3.10. Analyse des vulnérabilités (conception, construction…)

2.3.10.1. Liste des vulnérabilités connues

Il n'a pas été identifié de vulnérabilités connues sur ce produit particulier.

2.3.10.2. Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Hormis la possibilité de déni de service sur l'UTL, aucune vulnérabilité n'a été découverte pour un attaquant du niveau visé par la CSPN.

2.3.11. Accès aux développeurs

Au cours de l'évaluation, les évaluateurs ont eu accès au développeur du produit. Au cours des échanges techniques qui ont eu lieu, le développeur a fait preuve d'une très bonne maîtrise de son produit et a été en mesure de répondre rapidement aux questions posées.

2.3.12. Analyse de la facilité d'emploi et préconisations

2.3.12.1. Cas où la sécurité est remise en cause

Néant.

2.3.12.2. Recommandations pour une utilisation sûre du produit

Pour une utilisation sûre du produit, il est recommandé d'activer le mécanisme de sécurité anti-arrachement dès le chargement d'une clé secrète différente de la clé par défaut et/ou du chargement des clés RFID.

L'UTL doit héberger un système d'exploitation à jour concernant les correctifs de sécurité et être correctement administré. Le poste doit être durci afin d'être protégé contre des codes malveillants (voir le guide d'hygiène informatique [GUIDES-ANSSI], notamment ses règles 14 et 15).

De plus, l'installation et l'exploitation du dispositif doivent être effectuées conformément aux bonne pratiques décrites dans le guide de sécurité des technologies sans-contact pour le contrôle des accès physiques [GUIDES-ANSSI], notamment dans ses chapitres 6 et 7.

Enfin, pour assurer une sécurité de l'ensemble du dispositif mettant en œuvre ce produit, les fonctionnalités d'identification et d'authentification des badges doivent également avoir fait l'objet d'une certification à un niveau approprié au contexte d'utilisation (une certification EAL.4 augmentée du composant AVA_VAN.5 peut par exemple couvrir ce besoin).

2.3.12.3. Avis d’expert sur la facilité d’emploi

Moyennant le respect des recommandations évoquées précédemment, l’évaluateur n’a pas identifié de cas où le produit serait configuré ou utilisé de façon non sûre mais qu’un utilisateur pourrait raisonnablement croire sûre.

2.3.12.4. Notes et remarques diverses

Néant.

2.4. Analyse de la résistance des mécanismes cryptographiques

La liste de référence des mécanismes cryptographiques est celle fournie par la cible de sécurité [CDS] et les spécifications cryptographiques [SPEC_CRY]. La résistance de ces mécanismes a été analysée par l’évaluateur. Les résultats obtenus ont fait l’objet d’un rapport d’analyse [RTE] et concluent que, si les recommandations présentes dans [GUIDES] sont appliquées, les mécanismes analysés atteignent le niveau standard défini dans le référentiel cryptographique de l’ANSSI (voir [REF-CRY]).

2.5. Analyse du générateur d’aléas

Le produit évalué offre un générateur d’aléas qui utilisé par le logiciel embarqué. Les moyens mis en œuvre pour la génération et le retraitement des nombres aléatoires qui sont utilisés dans le lecteur permettent d’atteindre le niveau de résistances aux attaques visé par la CSPN.

3. La certification

3.1. Conclusion

L’évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l’impartialité requises pour un centre d’évaluation agréé.

Ce certificat atteste que le produit « Lecteur RFID LXS W33-E/PH5-7AD, version 1.0 » soumis à l’évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d’évaluation attendu lors d’une certification de sécurité de premier niveau.

3.2. Restrictions d’usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L’utilisateur du produit certifié devra s’assurer du respect des objectifs de sécurité sur l’environnement d’exploitation spécifiés dans la cible de sécurité [CDS] et suivre les recommandations énoncées dans le présent rapport.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN - Lecteur LXS-W33-E/Ph5-7AD ;* Référence : *CSPN-cible-Lecteur LXS-W33-E* ; Date : *27 mars 2012.*
[RTE]	*SPICA - Rapport Technique d'Evaluation ;* Référence : *LETI.CESTI.SPI.ETR-v1.2* ; Date : *6 mars 2013.*
[SPEC-CRY]	*CSPN - Fournitures cryptographiques ;* Version : *1.1* ; Référence : *CSPNFournitureCrypto-LecteursLXS-E* ; Date : *4 mars 2013.*
[GUIDES]	Guide d'utilisation : *CSPN - Guide d'utilisation SSCP V2 ;* Référence : *CSPNGuideSSCP-LecteursLXS-W33-Ev10* ; Date : *27 mars 2012.* Guide d'administration : *Manuel d'utilisation librairie du protocole SSCP2 ;* Référence : *MANU_SSCP2libMifareGlobalV.0.9* ; Date : *9 septembre 2012.*



Annexe 2. Références à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 1, n° 1414/ANSSI/SR du 30 mai 2011. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1417/ANSSI/SR du 30 mai 2011. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1416/ANSSI/SR du 30 mai 2011. Documents disponibles sur www.ssi.gouv.fr
[REF-CRY]	Référentiel général de sécurité, version 1.0, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20. Documents disponibles sur www.ssi.gouv.fr
[GUIDES-ANSSI]	Guide d'hygiène informatique de l'agence nationale de la sécurité des systèmes d'information (ANSSI), version finalisée du 28 janvier 2013. Disponible sur www.ssi.gouv.fr/hygiene-informatique. Guide sur la sécurité des technologies sans-contact pour le contrôle des accès physique, version de travail 1.0 du 19 novembre 2012. Disponible sur www.ssi.gouv.fr.